X-Force Red

Our Mission: Hacking Anything to Secure Everything

X-Force Red: Better Than Mr. Robot

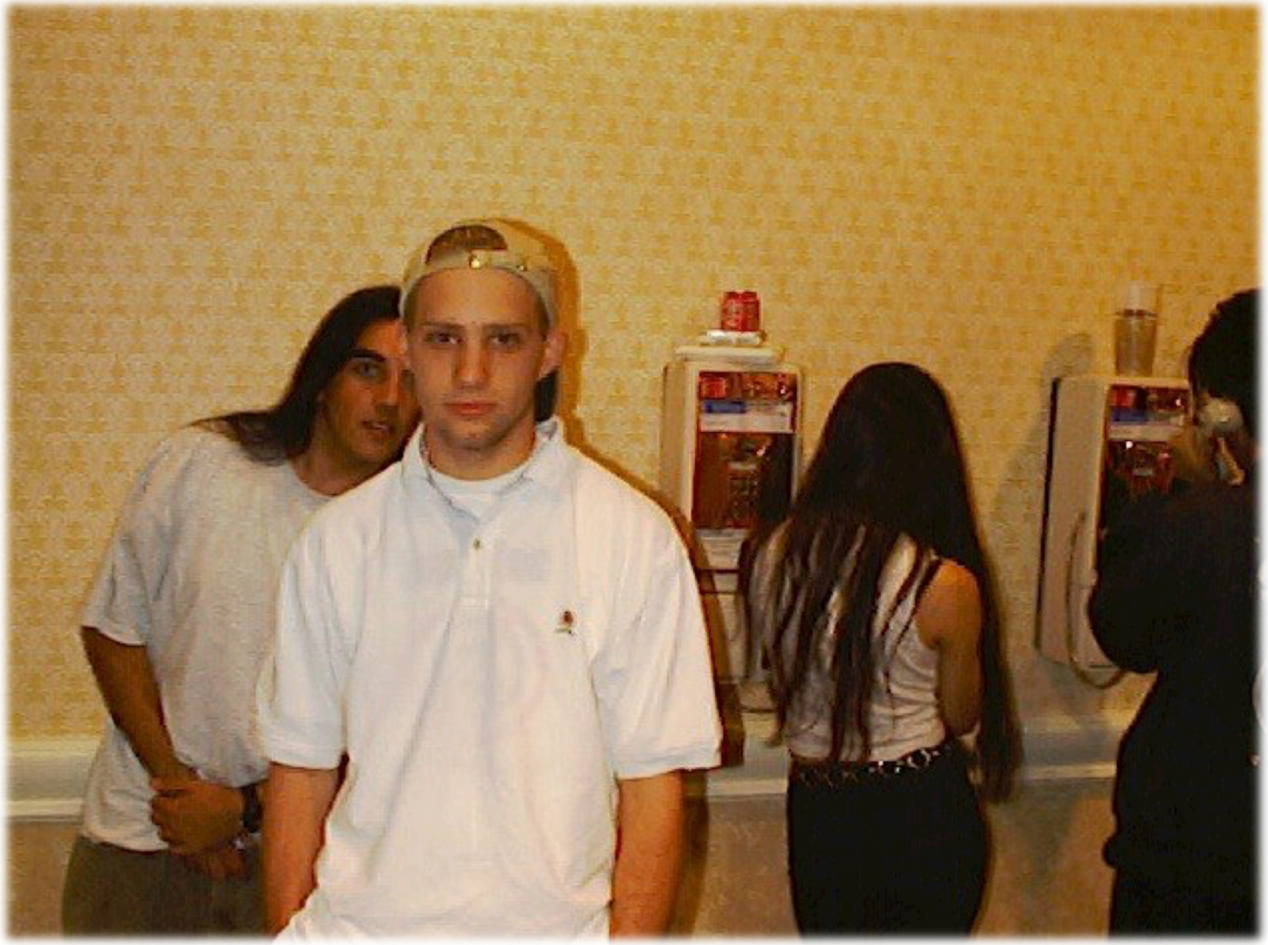
Charles Henderson
Global Managing Partner and Head of X-Force Red
Twitter: @angus_tx

A LITTLE BACKGROUND

Before it was a career…

DEF CON 4

Before there was Black Hat (circa 1996)



Steve Ocepek

This slide has nothing to do with this presentation (circa 2007)



Hacking is Solving a Series of Puzzles

Trying to make something do something it can’t

Getting to know a system so intimately you can work around its perceived limitations

Making the most of access rights and limited resources



Decisions

This is not a conscious decision but instead a moral compass



Mr. Robot – Why is this Interesting?

Somewhat believable, engrossing story about hacker mindset

Passion for understanding technology well enough to exploit it

”Companies are evil and security is impossible”



X-Force Red

SOME STORIES

Now that it is a career…

I run X-Force Red:

An autonomous team of veteran hackers, within IBM Security, hired to break into organizations and uncover risky vulnerabilities.

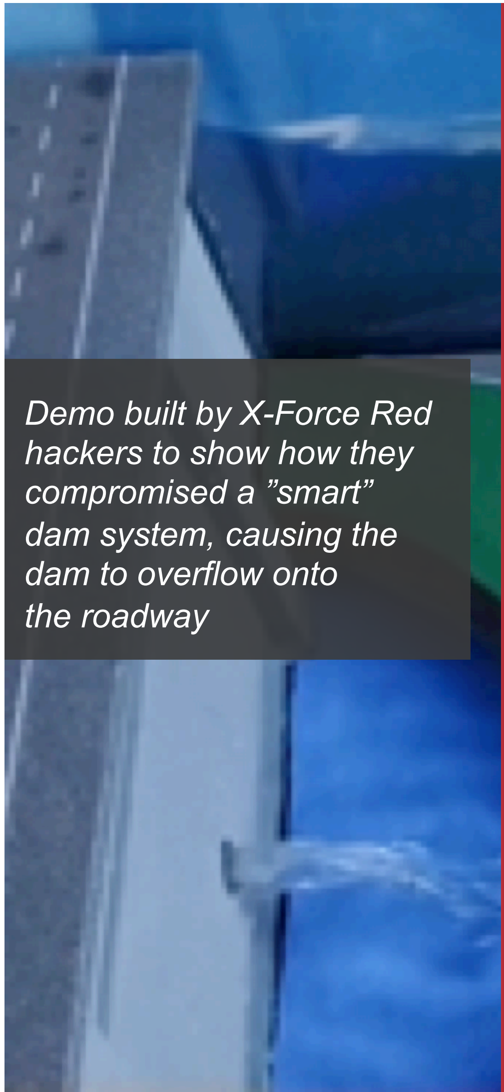
Offensive Security Services

- **Penetration testing**
- **Vulnerability management programs**
- **Red teaming**
- **Code review**
- **Static analysis**
- **Vulnerability assessments.**

This is X-Force Red



Some of the folks on my team:
Space Rogue | Evilmog | The Toymaker | Videoman | Q0phi |retBandit | keybored… and many more.



Demo built by X-Force Red hackers to show how they compromised a "smart" dam system, causing the dam to overflow onto the roadway

Smart City Security

My team found 17 zero-day vulnerabilities within four smart city products. Research unveiled at Black Hat USA 2018. Landed 100+ media stories worldwide.

BBC
WIRED
eWEEK
CNBC
Forbes
WSJ PRO CYBERSECURITY
THE PARALLAX YOUR EYE ON SECURITY NEWS
CNN
FOX BUSINESS
The Washington Post

Soooo, This Happened



A Problem Begins

I sold my car



Technology Abounds

Navigation System

Satellite Radio

Live Assist

Connected Car

Mobile Application



Mobile Application Features

Geolocation of Car

Climate Control

Navigation Control

Horn

Remote Unlock



The Sale

Traded car back to original factory dealer

I deauthorized all accounts, satellite radio, garage door openers, etc.

Dealer ensured that all keys issued to the car were surrendered at time of sale.



After The Sale

The Mobile App Still Worked...



...For Over Two Years

After The Sale: Demonic Possession



Everyone Loves Donuts

For most people, security is a secondary impulse.



X-Force Red

Offensive to a Defense Contractor

Try not to get shot



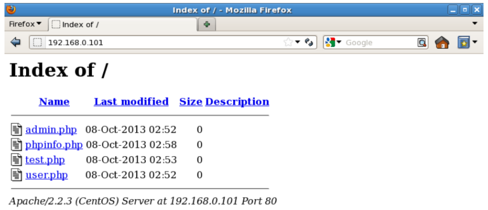
Offensive to a Defense Contractor

Try not to get shot



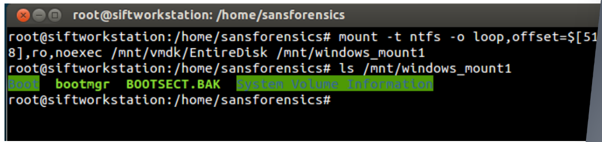
X-Force Red

Virtually Rich!





Sometimes a silly flaw can be made serious by context





X-Force Red

SOME ADVICE

Now that you have listened…

- THINK LIKE AN ATTACKER AND MODEL YOUR THREAT
- TEST EVERYTHING YOU CAN
- EVOLVE WITH CARE
- TEST MANUALLY TOO
- DON'T FORGET TO FIX WHAT YOU FIND

YOUR TURN

Questions?

twitter: @angus_tx

X-Force Red

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM®